

**THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON**

**ROTHSCHILD BROADCAST
DISTRIBUTION SYSTEMS, LLC,**

Plaintiff,

v.

SYNOLOGY AMERICA CORP.,

Defendant.

CIVIL ACTION NO. _____

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff Rothschild Broadcast Distribution Systems, LLC (“Plaintiff” or “Rothschild Broadcast Distribution Systems”) files this complaint against Synology America, Corp. (“Synology”) for infringement of U.S. Patent No. 8,856,221 (hereinafter the “221 Patent”) and alleges as follows:

PARTIES

1. Plaintiff is a Texas limited liability company with an office at 1801 NE 123 Street, Suite 314, Miami, FL 33181.
2. On information and belief, Defendant is a Washington corporation, with a place of business at 3535 Factoria Blvd. SE, Ste. 200, Bellevue, WA, 98006-1263. On information and belief, Defendant may be served through its agent, Chun-Pin Wang, at the same address.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, 35 U.S.C. § 271 et seq. Plaintiff is seeking damages, as well as attorney fees and costs.
4. Jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 (Federal Question) and 1338(a) (Patents).

5. On information and belief, this Court has personal jurisdiction over Defendant because Defendant has committed, and continues to commit, acts of infringement in this District, has conducted business in this District, and/or has engaged in continuous and systematic activities in this District.

6. Upon information and belief, Defendant's instrumentalities that are alleged herein to infringe were and continue to be used, imported, offered for sale, and/or sold in the District.

7. Venue is proper in this District under 28 U.S.C. §1400(b) because Defendant is deemed to be a resident in this District. Alternatively, acts of infringement are occurring in this District and Defendant has a regular and established place of business in this District.

BACKGROUND

8. On October 7, 2014, the United States Patent and Trademark Office ("USPTO") duly and legally issued the '221 Patent, entitled "System and Method for Storing Broadcast Content in a Cloud-Based Computing Environment" after the USPTO completed a full and fair examination. The '221 Patent is attached as Exhibit A.

9. Rothschild Broadcast Distribution Systems is currently the owner of the '221 Patent.

10. Rothschild Broadcast Distribution Systems possesses all rights of recovery under the '221 Patent, including the exclusive right to recover for past, present and future infringement.

11. The '221 Patent contains thirteen claims including two independent claims (claims 1 and 7) and eleven dependent claims.

COUNT ONE **(Infringement of United States Patent No. 8,856,221)**

12. Plaintiff refers to and incorporates the allegations in Paragraphs 1 - 11, the same as if set forth herein.

13. This cause of action arises under the patent laws of the United States and, in particular under 35 U.S.C. §§ 271, *et seq.*

14. Defendant has knowledge of its infringement of the '221 Patent, at least as of the service of the present complaint.

15. Upon information and belief, Defendant has infringed and continues to infringe one or more claims, including at least Claim 7, of the '221 Patent by making, using, importing, selling, and/or offering for media content storage and delivery systems and services covered by one or more claims of the '221 Patent.

16. Accordingly, Defendant has infringed, and continues to infringe, the '221 Patent in violation of 35 U.S.C. § 271.

17. Defendant sells, offers to sell, and/or uses media content storage and delivery systems and services, including, without limitation, the Synology surveillance station video monitoring and management platform, and any similar products ("Product"), which infringes at least Claim 7 of the '221 Patent.

18. The Product practices a method of storing (e.g., cloud storage) media content (e.g., video, audio, etc.) and delivering requested media content (streaming video) to a consumer device (e.g., mobile device with app). Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.

Surveillance Station

Protect your business, home, and other environments with reliable, intuitive Surveillance Station, delivering intelligent monitoring and video management tools to safeguard your valuable assets.



Live View & Alert

Monitor video streams from multiple cameras in real time and set up smart analytics to catch suspicious behavior.



Recording & Playback

Manage, analyze, export, or play recordings with an intuitive interface.



Mobile

Besides your PC, you can also use iOS, or Android™ mobile device to monitor anytime, anywhere. [Learn more](#)

Source: <https://www.synology.com/en-global/surveillance/overview>

Recording & Playback

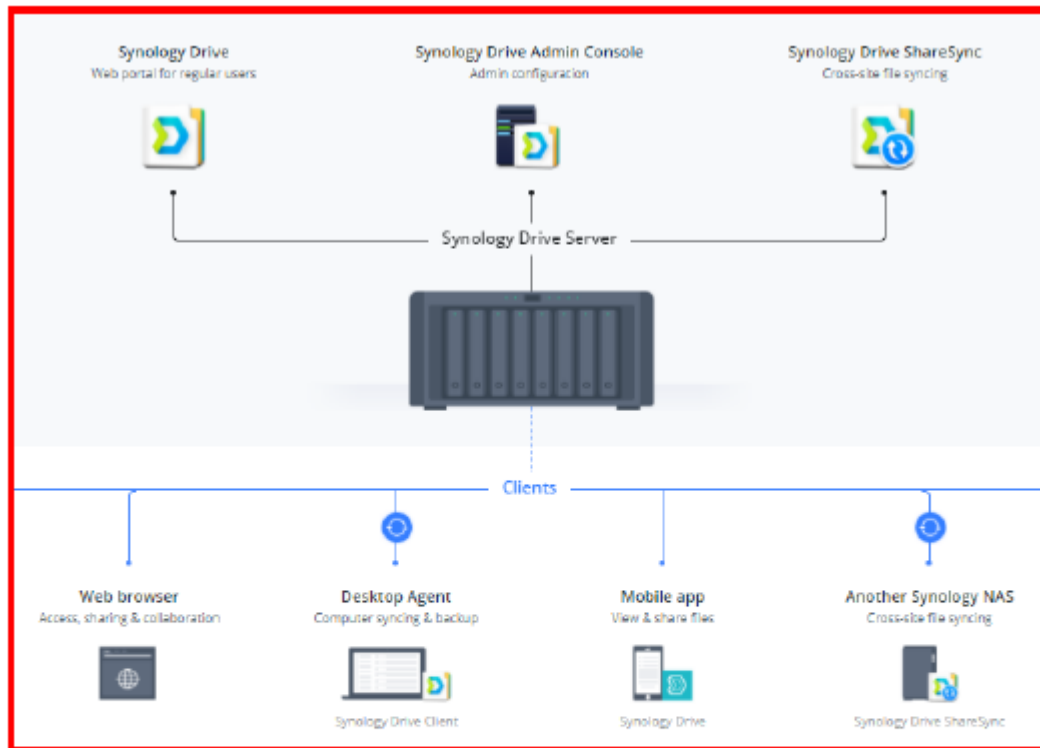
Set up a variety of recording modes according to your requirements and compare footage recorded from different cameras simultaneously. You can also analyze events in the Smart Search app, and ensure the reliability of exported files with Synology Evidence Integrity Authenticator.

Source: https://www.synology.com/en-global/surveillance/feature/recording_playback

Powerful private cloud storage with no recurring fees

With large storage capacities from one to hundreds of terabytes (depending on your choice of Synology NAS and hard drives), Synology Drive makes files readily available whenever and wherever you need them.

Source: <https://www.synology.com/en-global/dsm/feature/drive>



Source: <https://www.synology.com/en-global/dsm/feature/drive>

Quota limitation:

- The maximum storage usage quota that can be entered for each user is approximately 4 TB (4095 GB).

Source: https://www.synology.com/en-global/knowledgebase/DSM/help/DSM/AdminCenter/file_user_create



Source: https://www.synology.com/en-us/solution/smart_home_surveillance

19. The Product necessarily includes a receiver configured to receive a request message including data indicating requested media content (e.g., the Product must have infrastructure to receive a request to store recorded media content or to stream recorded media content on a smartphone; additionally, the request message must contain data that identifies the content to be stored or streamed) and a consumer device identifier corresponding to a consumer device (e.g., the user credentials are used to access the contents of the Product). Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.

Create File Requests

File requests are file-uploading invitations sent to non-DSM users. With file request links, non-DSM users can directly upload multiple files to File Station on your Synology NAS, without the need of owning corresponding user accounts and file-uploading privileges.

To create file request links:

1. Go to **File Station** and select a folder as the upload destination.
2. Click **Action** or right-click the destination folder, and select **Create file request**.
3. In the pop-up window, you can find/modify the information below:
 - **File path**: List the destination directory path.
 - **Link**: List the file request link to share with target users.
 - **Your name**: Enter a name to indicate requestor identity. The default value is your username.
 - **Message**: Customize the message for target users.
 - **Enable password protection**: Select this option so that only users with the password can upload files via the created link. Specify the password in the box below.
 - **Validity period**: Click this button to customize the duration of this file request link:
 - **Set up stop time**: Select this option to determine by date and time when the link stops to work for file uploading.
 - **Set up start time**: Select this option to determine by date and time when the link starts to work for file uploading.
 - **Number of allowed access**: Select this option to determine how many times the link can be accessed.
4. Click **Save** to finish the settings.

Source: https://www.synology.com/en-global/knowledgebase/DSM/help/FileStation/file_request

To share file request links:

To find the file request URL, go to **File Station > Tools > Shared Links Manager** and double-click the desired link. You can share the link in either way below:

- Simply copy the URL to target users.
- Send out the link via **the Default Email** (your DSM email account) or via **Mail** (a third-party email application). For first-time users, follow the wizard's instructions to set up an email account for use.

To upload files:

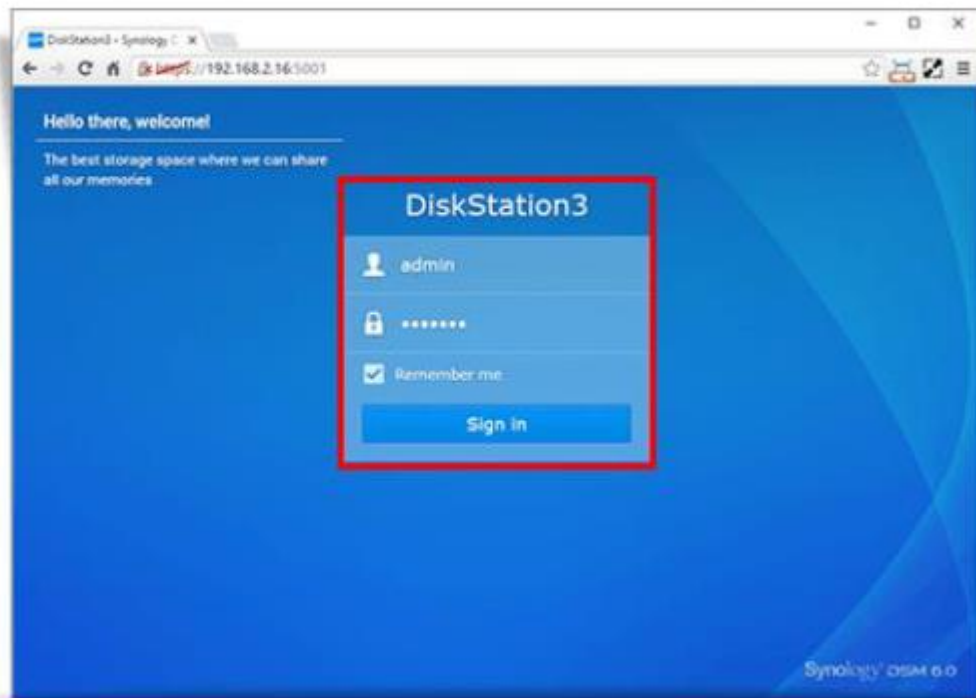
If you are requested to upload files via the link, please do as follows:

1. Open the given URL on the local computer or a mobile device (Android or iOS). Enter the password if it is required.
2. On the upload page, enter a name that indicates your identity.
3. Simply drag and drop the file(s) to upload, or click **Add Files** to select file(s).
4. Click **Upload** to finish the request.


Source: https://www.synology.com/en-global/knowledgebase/DSM/help/FileStation/file_request

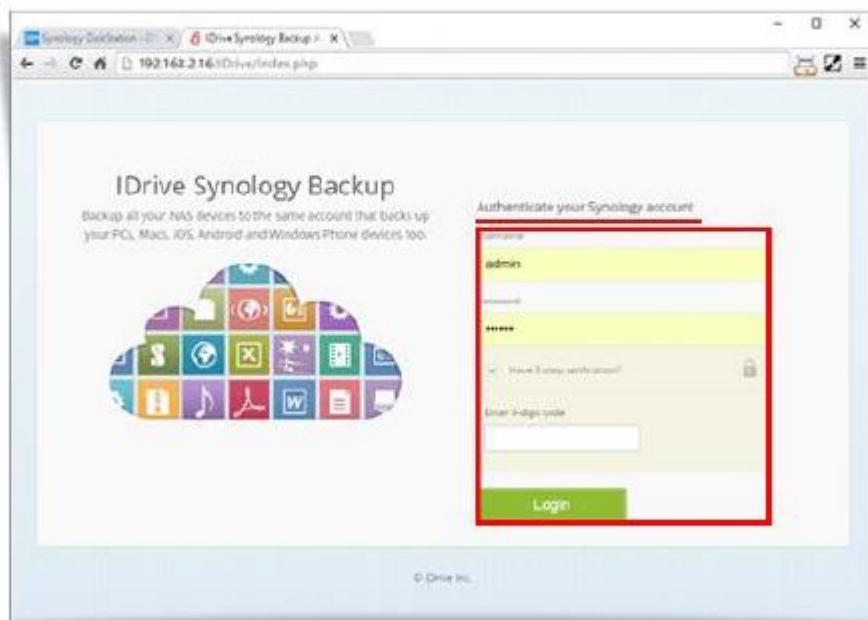
Steps to log in to the Synology Backup app,

1. Login to the Synology NAS device with your credentials.



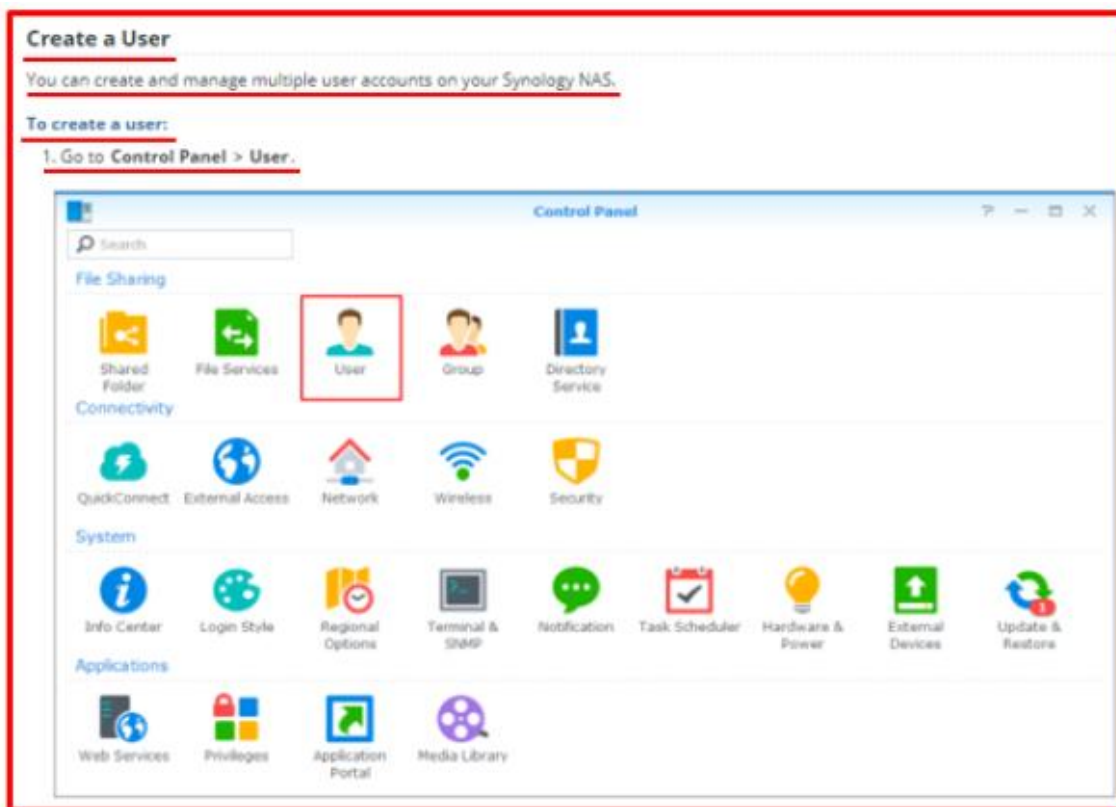
Source: <https://www.idrive.com/help/synology/login>

2. To launch the app, click  on the application gallery.
3. Enter your NAS device credentials and click **Login**.
4. Enter the 6-digit code, if you had set up the 2-step verification with your NAS device.



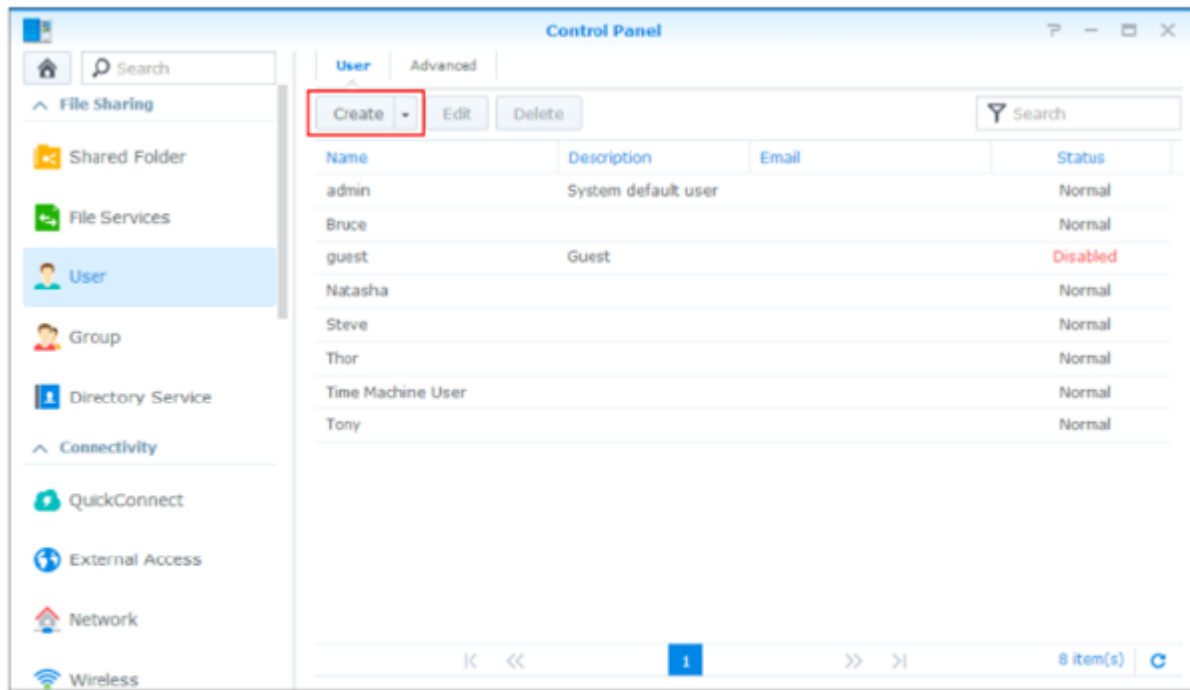
Source: <https://www.idrive.com/help/synology/login>

20. The Product necessarily determines whether the consumer device identifier corresponds to the registered consumer device (e.g., a user must be a registered user to access the Product's services). Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.



Source: https://www.synology.com/en-global/knowledgebase/DSM/help/DSM/AdminCenter/file_user_create

2. Click the **Create** button and then Create user. This action launches the **User Creation Wizard**.



Source: https://www.synology.com/en-global/knowledgebase/DSM/help/DSM/AdminCenter/file_user_create

21. The Product provides for both media downloads and/or storage, and media streaming. After a successful login, the Product necessarily determines whether the request received from a customer is a request for storage (e.g., recording or storing content) or content (e.g., streaming of media content). Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.

Syncing on demand

Save the disk space and bandwidth of your PC with On-demand Sync¹. See all your files in the synced folders, yet they're only streamed to the desktop when you open them. Of course, you can always exclude certain subfolders, file formats or put a limit on the file size.

Synology Drive

Now, Synology makes it possible for every home and office to host your own cloud – with 100% data ownership and no subscription fees. See how this changes the way we live and work, access and share data.

Source: <https://www.synology.com/en-global/dsm/feature/drive>

Powerful private cloud storage with no recurring fees

With large storage capacities from one to hundreds of terabytes (depending on your choice of [Synology NAS](#) and hard drives), [Synology Drive](#) makes files readily available whenever and wherever you need them.

Source: <https://www.synology.com/en-global/dsm/feature/drive>

22. The Product verifies that media content identified in the media data of the storage request message (e.g., request to record content) is available for storage in order to prevent data errors that would result from attempting to store content that is not available for storage. The Product must verify that the media content (e.g. specific recording) identified in the media data of the storage request message is available for storage in order to prevent data errors that would result from attempting to store content that is not available for storage (e.g., the product must verify a user's ability to store media content is limited to a certain amount of time). If any media content is streamed the user has the option to upload it to cloud storage. Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.

To share file request links:

To find the file request URL, go to **File Station > Tools > Shared Links Manager** and double-click the desired link. You can share the link in either way below:

- Simply copy the URL to target users.
- Send out the link via **the Default Email** (your DSM email account) or via **Mail** (a third-party email application). For first-time users, follow the wizard's instructions to set up an email account for use.

To upload files:

If you are requested to upload files via the link, please do as follows:

1. Open the given URL on the local computer or a mobile device (Android or iOS). Enter the password if it is required.
2. On the upload page, enter a name that indicates your identity.
3. Simply drag and drop the file(s) to upload, or click **Add Files** to select file(s).
4. Click **Upload** to finish the request.

Source: https://www.synology.com/en-global/knowledgebase/DSM/help/FileStation/file_request

To set recording archive settings, configure any of the following:

- **Customize archive folder name:** Enter a name for the recording archive folder that will be used to save the recorded videos.
- **Customize file name prefix:** Enter the file name prefix that will appear in front of each file name.
- **Recording Storage:** Select a recording storage to be used to save the recorded videos.

Source: https://www.synology.com/en-global/knowledgebase/Surveillance/help/SurveillanceStation/recording_settings_recording

23. If a customer requests content (e.g., live streaming of media content), then a processor within the Product necessarily initiates delivery of the content to the customer's device. The Product will initiate delivery of the requested media content to the consumer device (e.g., stream media content feed to a smartphone or tablet etc.) if the request message is a content request message (e.g., request for live streaming). Certain aspects of these elements are illustrated in the screen shots below and/or in screen shots provided in connection with other allegations herein.

Live View

You can use Live View as a centralized interface for viewing live video from different cameras. Live View provides many different features to help perform real-time surveillance including:

- Simultaneously watch up to 100 channels of live video
- Take snapshots
- Adjust the camera angle
- Create camera groups to easily manage large numbers of cameras
- Customize channel layouts according to your needs
- Switch live view stream profiles according to your needs
- Integrate cameras hosted on different recording servers using Central Management System (CMS)

In addition, live-view alerts lets you track targets during live video viewing and recording. You can choose from several alert events for your IP cameras, and track suspicious events intelligently to trigger smart recording on-the-fly. Click [here](#) to learn how to use Live View or see [here](#) for more information about Alerts.

Source: https://www.synology.com/en-global/knowledgebase/Surveillance/help/SurveillanceStation/liveview_desc

24. The media data includes time that indicates a length of time to store the requested media content. For example, a user is allowed to store media content of certain time period. Uploading media content to storage will depend on the time period or size of that particular media content. Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.

Recording

In the **Recording** tab, you can configure recording and archiving settings.

To set recording settings, configure any of the following:

- **Pre-recording time/Post-recording time:** Set how much time the recording will extend backwards/forwards when events are detected.
Note: Increasing the pre-recording and post-recording times can help record triggered events more completely. For example, suppose you set both at 5 seconds and your camera detects an event that lasts 10 seconds. The footage of the 5 seconds prior to and the 5 seconds after the event will also be included in the detection results, giving you 20 seconds of footage in total.
- **Keep the files within (days):** Specify a period of time (in days) within which you wish to retain the recordings. Any recordings that were saved earlier than the specified time range will be deleted automatically.
- **Limit the archive folder up to (GB):** Specify the maximum size limit (in gigabytes) of the storage space to archive recordings. The oldest recordings will be overwritten by new ones when the specified maximum size limit is reached.
- Click **Estimate Required Space** to get the estimated storage space that the camera may need for continuous recording with its current settings.

Note:

- The pre-recording time is related to memory consumption. The test shown on the Synology official website is conducted based on a 5-second pre-recording time. If you set up the pre-recording time to be longer than the default pre-recording time, then the maximum number of IP cameras supported for your NAS will be affected due to the increase in memory consumption.
- If **Keep the files within (days)** and **Limit the archive folder up to (GB)** are applied simultaneously, files will be rotated once either of the thresholds is exceeded. For example, if you decided to keep the recordings within 60 days and limit the archive storage up to 15 GB, there is a chance that older recordings will be overwritten before being kept for 60 days once the accumulated file size surpasses 15 GB.

Note:

- Only the shared folders created by Surveillance Station can be set as recording storage. Please refer to **Recording > Storage** in Surveillance Station Help for more information.
- When you click **Save** to complete the changing of recording storage, the status of the camera will become "Configuring". During the time of configuration, live view and recording can work normally, but you cannot edit the camera until the configuration is finished. The time needed for configuration depends on the size of the camera's recorded videos.
- If the recording storage of your camera crashed or no longer exists, the status of your camera will become **Storage unavailable**, and all of its recording functions will stop. You will need to select another recording storage for the camera to work normally again.
- External devices are not supported as recording storages.

Source: https://www.synology.com/en-global/knowledgebase/Surveillance/help/SurveillanceStation/recording_settings_recording

25. The Product must first determine whether the requested media content exists prior to initiating delivery in order to prevent data errors that would result from attempting to transmit media content that does not exist (e.g. the product must verify that a particular requested data is stored in the cloud). Also, the processor (i.e. the processor of mobile devices with the app) is configured to determine whether the media content exists (i.e. user can search the archived media content and processor can identify the existence of that particular media content). Certain aspects of these elements are illustrated in the screenshots below and/or in those provided in connection with other allegations herein.

Syncing on demand

Save the disk space and bandwidth of your PC with On-demand Sync¹. See all your files in the synced folders, yet they're only streamed to the desktop when you open them. Of course, you can always exclude certain subfolders, file formats or put a limit on the file size.

Powerful private cloud storage with no recurring fees

With large storage capacities from one to hundreds of terabytes (depending on your choice of Synology NAS and hard drives), Synology Drive makes files readily available whenever and wherever you need them.

Source: <https://www.synology.com/en-global/dsm/feature/drive>

To set recording archive settings, configure any of the following:

- **Customize archive folder name:** Enter a name for the recording archive folder that will be used to save the recorded videos.
- **Customize file name prefix:** Enter the file name prefix that will appear in front of each file name.
- **Recording Storage:** Select a recording storage to be used to save the recorded videos.

Source: https://www.synology.com/en-global/knowledgebase/Surveillance/help/SurveillanceStation/recording_settings_recording

26. After the processor determines whether the requested media content is available, it determines whether there are restrictions associated with the requested media content (e.g., user access restrictions, subscription, etc.). Certain aspects of these elements are illustrated in the screenshots below and/or those provided in connection with other allegations herein.

Syncing on demand

Save the disk space and bandwidth of your PC with On-demand Sync¹. See all your files in the synced folders, yet they're only streamed to the desktop when you open them. Of course, you can always exclude certain subfolders, file formats or put a limit on the file size.

Powerful private cloud storage with no recurring fees

With large storage capacities from one to hundreds of terabytes (depending on your choice of [Synology NAS](#) and hard drives), [Synology Drive](#) makes files readily available whenever and wherever you need them.

Source: <https://www.synology.com/en-global/dsm/feature/drive>

To set recording archive settings, configure any of the following:

- **Customize archive folder name:** Enter a name for the recording archive folder that will be used to save the recorded videos.
- **Customize file name prefix:** Enter the file name prefix that will appear in front of each file name.
- **Recording Storage:** Select a recording storage to be used to save the recorded videos.

Source: https://www.synology.com/en-global/knowledgebase/Surveillance/help/SurveillanceStation/recording_settings_recording

Manage Advanced Shared Folder Permissions

The page at **Control Panel > Shared Folder > Edit > Advanced** includes the below options in order to further fine-tune the access permissions of a shared folder.

Advanced Share Permissions

Advanced share permissions offer an additional layer of control to manage the access permissions of shared folders. When enabled, users and groups can view or modify the contents of a shared folder only if the user or group has been granted both advanced share permissions and Windows ACL permissions (located at **Shared Folder > Edit > Permissions**).

To enable advanced share permissions:

1. Tick the box **Enable advanced share permissions**.
2. Click **Advanced Share Permissions** to modify the advanced share permissions for the shared folder.

Note:

- Advanced share permissions are applied when a user accesses a shared folder via the following file services: Windows File Sharing, Apple File Sharing, File Station, FTP, and WebDAV.

Advanced Settings

If necessary, you can place further restrictions on users when they access a shared folder via File Station, FTP, or WebDAV.

- **Disable directory browsing:** Enabling this option restricts users from viewing the contents of the shared folder.
- **Disable modification of existing files:** Enabling this option restricts users from moving, deleting, or modifying files in the shared folder. Please note users will still be able to view, download/upload, copy, or unzip the contents of the shared folder.
- **Disable file downloading:** Enabling this option restricts users from downloading the contents of the shared folder.

Source: https://www.synology.com/en-global/knowledgebase/DSM/help/DSM/AdminCenter/file_share_privilege.asp

27. Defendant's actions complained of herein will continue unless Defendant is enjoined by this Court.

28. Defendant's actions complained of herein is causing irreparable harm and monetary damage to Plaintiff and will continue to do so unless and until Defendant is enjoined and restrained by this Court.

29. The '221 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

30. A copy of the '221 Patent, titled "System and Method for Storing Broadcast Content in a Cloud-based Computing Environment," is attached hereto as Exhibit A.

31. By engaging in the conduct described herein, Defendant has injured Plaintiff and is liable for infringement of the '221 Patent, pursuant to 35 U.S.C. § 271.

32. Defendant has committed these acts of literal infringement, or infringement under the doctrine of equivalents of the '221 Patent, without license or authorization.

33. As a result of Defendant's infringement of the '221 Patent, injured Plaintiff has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate for Defendant's past infringement, together with interests and costs.

34. Plaintiff is in compliance with 35 U.S.C. § 287.

35. As such, Plaintiff is entitled to compensation for any continuing and/or future infringement of the '221 Patent up until the date that Defendant ceases its infringing activities.

DEMAND FOR JURY TRIAL

36. Rothschild Broadcast Distribution Systems, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks the Court to:

- (a) Enter judgment for Plaintiff on this Complaint on all cases of action asserted herein;
- (b) Enter an Order enjoining Defendant, its agents, officers, servants, employees, attorneys, and all persons in active concert or participation with Defendant who receives notice of the order from further infringement of United States Patent No. 8,856,221 (or, in the alternative, awarding Plaintiff running royalty from the time judgment going forward);
- (c) Award Plaintiff damages resulting from Defendants infringement in accordance with 35 U.S.C. § 284;
- (d) Award Plaintiff such further relief to which the Court finds Plaintiff entitled under law or equity.

Dated: March ____, 2021

Respectfully submitted,

/s/

BRIAN HOLLOWAY

Washington State Bar: 57100

HOLLOWAY IP

5544 25th Avenue NE

Seattle, Washington, 98501

(206) 453-8357

Brian@hollowayip.org

OF COUNSEL

JAY JOHNSON (*Pro Hac Vice Application Pending*)

State Bar No. 24067322

KIZZIA JOHNSON, PLLC

1910 Pacific Avenue, Suite 13000

Dallas, Texas 75201

(214) 451-0164

Fax: (214) 451-0165

Jay@kpcllc.com

ATTORNEYS FOR PLAINTIFF